



KING COUNTY
IT SECURITY ANALYST
INFORMATION TECHNOLOGY PROJECT MANAGER II
OFFICE OF INFORMATION RESOURCE MANAGEMENT
Annual Salary Range: \$78,335 – \$99,294
Job Announcement: 06CY6066
OPEN: 5/8/06 CLOSE: Open Until Filled

WHO MAY APPLY: This position is open to the general public. This is an eight month term-limited temporary position that is fully benefited (medical, dental, vision, etc.). The term may be extended based on funding resources.

WHERE TO APPLY: Required application materials can be mailed to: **Terra Strouhal, 701 Fifth Avenue, Suite 3460, Seattle, WA 98104. Fax (206) 205-0725.** Email applications are encouraged at oirmrecruit@metrokc.gov All application materials must be included. Applications materials must be received by 4:30 p.m. on the closing date. Postmarks are not accepted. Please note: Applications not received at the locations specified above and those that are not complete may not be processed.

FORMS AND MATERIALS REQUIRED:

- King County application form. Application forms may be found at <http://www.metrokc.gov/ohrm/jobs/JobApplications.htm>
- Resume
- A letter of interest detailing your background and describing how you meet or exceed the requirements.

WORK LOCATION: 701 Fifth Avenue, Bank of America Tower, Downtown Seattle, WA.

WORK SCHEDULE: This position is exempt from the provisions of the Fair Labor Standards Act, and is not overtime eligible. The workweek is normally Monday through Friday.

POSITION SUMMARY: King County requires a senior information security person with a strong technology background to lead the development of the King County's IT Risk Management program. As a member of the Information Security and Privacy program, this person will work with staff across the county, through the county's technology governance process and directly with technology staff in county agencies. The selected candidate will also be responsible for selecting, planning deployment, and overseeing deployment of the security controls to meet the needs of King County and the 15 independent information technology groups. This person will use their expertise in network and host security and in project management to plan and oversee the selection and deployment of selected security controls countywide. This position will have no direct reports. It will work with and report to the Chief Information Security and Privacy Officer.

PRIMARY JOB DUTIES INCLUDE: The Information Security and Privacy program needs a Security Analyst to be part of the project team to complete work in the following areas:

- Support the development of King County's IT risk management program.
 - Assist in the development of an IT risk management framework
 - Assist in the development of all forms and documentation associated with IT risk management
 - Assist in the development of risk management training for both technical and non-technical staff

- Coordinate the evaluation, selection, and deployment of an electronic risk management system.
- Security and privacy controls selection and deployment project including:
 - Research, of security and privacy controls
 - Product selection and contracting
 - Countywide deployment planning
 - Oversee agency deployment efforts
- Security policies, standards and guideline development and review
- Assist in the development of information security awareness efforts.
- Make presentations to technical, non-technical and management audiences.
- Create written reports, drawings and documentation in support of the Information Security and Privacy program.
- Conduct research on emerging products, services, protocols, and standards.
- Recommend and deploy additional security products and tools, or enhancements to existing tools, to detect violations of network security measures.
- Other duties as assigned.

QUALIFICATIONS:

- Four years of experience directly related to information technology security. This experience should include active participation in security programs and processes that have contributed to the development and administration of an organization wide IT security architecture.
- Bachelor's degree in Computer Science, Engineering, Business, or related discipline is desired.
- Strong ability to implement network, system, and organizational security practices, policies, and procedures based on accepted industry standards such as ISO 17799, NIST and COBIT.
- Understanding of information technologies, specifically security technologies including firewalls, virtual private networks, intrusion detection/prevention, encryption, and access control.
- Working technical knowledge of current systems software, operating systems, and PC protocols and standards.
- Experience in IT risk management including risk analysis processes and models, risk mitigation, documentation and facilitation of risk evaluation work sessions.
- Knowledge of applicable laws and practices relating to information privacy and security.
- Ability to conduct research into security issues and products as required.
- Ability to implement information security systems, solutions, and practices.
- Good working knowledge of business and/or systems analysis.
- Demonstrated ability to apply analytical and problem-solving skills to information security and privacy issues.
- Project management skills that include planning and deploying security controls.
- Ability to effectively communicate both verbally and in writing to both technical and non-technical staff on issues of information security and privacy. The ability to write documents ranging from formal and informal reports, system documentation, and training materials. Must be able to prepare these materials with limited advance notice.
- The ability to work with limited supervision and limited direction.
- Demonstrated ability to work effectively in a collaborative team environment.
- The ability to prioritize and execute tasks in crisis situation.
- The demonstrated ability to apply effective organizational skills and excellent attention to detail.
- Ability to work with vendors and independent contractors to develop solutions and recommendations.

LICENSING/CERTIFICATION REQUIREMENTS:

- CISSP and/or CISM certification highly desirable.
- Training on ISO 17799 or NIST standards is preferred.

NECESSARY SPECIAL QUALIFICATIONS: The applicant selected for this position may be required to pass a background investigation.

SELECTION PROCESS: Applications will be screened for qualifications. Competitive applicants will be invited to an interview. Finalists may be asked to complete a post interview research exercise. Salary will depend on qualifications.

UNION REPRESENTATION: This position is not currently represented by a union.

CLASS CODE: 736401